

GAO

Report to the Committee on Armed
Services, Special Oversight Panel on
Department of Energy Reorganization
House of Representatives

March 2002

NUCLEAR SECURITY

Lessons to Be Learned from Implementing NNSA's Security Enhancements



G A O

Accountability * Integrity * Reliability

Report Documentation Page

Report Date 00MAR2002	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle NUCLEAR SECURITY: Lessons to Be Learned from Implementing NNSAs Security Enhancements	Contract Number	
	Grant Number	
	Program Element Number	
Author(s)	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) General Accounting Office, PO Box 37050, Washington,DC 20013	Performing Organization Report Number GAO-02-358	
Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)	
	Sponsor/Monitor's Report Number(s)	
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract In the late 1990s, a number of incidents at nuclear weapons facilities highlighted important security weaknesses at the Department of Energy (DOE). ¹ To address these weaknesses, DOE has developed numerous initiatives to improve nuclear security. The initiatives cover a broad range of security areas: physical security, personnel security, information security, cyber security, and counterintelligence. Some of these initiatives require the creation of new offices and new policies, while others require the development of programs and processes meant to address specific weaknesses. In addition, the Congress sought to improve nuclear security by creating the National Nuclear Security Administration (NNSA) on March 1, 2000, as a separately organized agency within DOE. As a result of the September 11, 2001, terrorist attacks, improving security has taken on a higher priority given the sensitivity and hazards of the work that DOE and NNSA perform.		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract SAR	

Number of Pages

39

Contents

Letter		1
	Results in Brief	3
	Background	5
	DOE and NNSA Have Implemented Many Initiatives, and Lessons Can Be Learned to Improve Future Initiatives	7
	NNSA Has Begun to Develop a Security Structure and Program, but Key Issues Need to Be Addressed	12
	Conclusions	19
	Recommendations for Executive Action	20
	Agency Comments and Our Evaluation	20

Appendix I	Scope and Methodology	23
-------------------	------------------------------	-----------

Appendix II	Status of Initiatives to Improve Nuclear Security at DOE and NNSA	25
--------------------	--	-----------

Appendix III	Comments from the Department of Energy and the National Nuclear Security Administration	30
---------------------	--	-----------

Related GAO Products		35
-----------------------------	--	-----------

Table		
	Table 1: Status of DOE/NNSA Security Initiatives	8

Abbreviations	
DOE	Department of Energy
FBI	Federal Bureau of Investigation
FV&A	Foreign Visits and Assignments
NEST	Nuclear Emergency Search Team
NNSA	National Nuclear Security Administration



United States General Accounting Office
Washington, DC 20548

March 29, 2002

The Honorable Mac Thornberry
Chairman
The Honorable Ellen Tauscher
Ranking Minority Member
Committee on Armed Services
Special Oversight Panel on
Department of Energy Reorganization
House of Representatives

In the late 1990s, a number of incidents at nuclear weapons facilities highlighted important security weaknesses at the Department of Energy (DOE).¹ To address these weaknesses, DOE has developed numerous initiatives to improve nuclear security. The initiatives cover a broad range of security areas—physical security, personnel security, information security, cyber security, and counterintelligence. Some of these initiatives require the creation of new offices and new policies, while others require the development of programs and processes meant to address specific weaknesses. In addition, the Congress sought to improve nuclear security by creating the National Nuclear Security Administration (NNSA) on March 1, 2000, as a separately organized agency within DOE. As a result of the September 11, 2001, terrorist attacks, improving security has taken on a higher priority given the sensitivity and hazards of the work that DOE and NNSA perform.

NNSA is responsible for maintaining and enhancing the safety, reliability, and performance of the nation's nuclear weapons; maintaining the nation's ability to design, produce, and test nuclear weapons; preventing the proliferation of weapons of mass destruction; and designing, building, and maintaining naval nuclear propulsion systems. In creating NNSA, the Congress directed it to develop its own program to protect nuclear materials and information under its purview and created the Office of Defense Nuclear Security to oversee the implementation of security policies and procedures and the Office of Defense Nuclear

¹ In this report, the term “security” will be used to include both security and counterintelligence unless a distinction is necessary for clarity. Both DOE and NNSA have separate security and counterintelligence offices.

Counterintelligence to gather information and conduct activities to protect against espionage and other intelligence-gathering activities.

Concerned about the security of the nation's nuclear weapons program, you asked us to assess the status of DOE's and NNSA's initiatives to improve security. As agreed with your offices, this report examines the extent to which (1) DOE and NNSA have implemented security initiatives at NNSA facilities and (2) NNSA has developed an organizational structure for security and a program to safeguard nuclear information and materials. At your request, we also looked at NNSA management issues and reported on these issues separately.²

We identified 75 nuclear security-related initiatives based on our review of presidential decision directives,³ announcements by the secretary of energy or other high-ranking department officials, and initiatives begun by DOE and NNSA security offices between February 1998 and January 2001.⁴ We did not assess whether these 75 initiatives addressed all security problems at DOE and NNSA. As part of our review, we visited selected sites that are representative of the various aspects of NNSA's work to determine whether initiatives were implemented. Specifically, we visited Lawrence Livermore National Laboratory, Sandia National Laboratories, the Pantex Plant, and the Bettis Atomic Power Laboratory. Lawrence Livermore, Sandia, and Pantex report to the Office of Defense Programs within NNSA. Bettis reports to the naval reactors program within NNSA. Naval reactors is a semiautonomous entity within NNSA, with a unique security structure and program. We also collected information on actions taken by DOE and NNSA in response to the September 11 terrorist attacks, but we did not evaluate the implementation of these actions. Currently, we have an ongoing assignment that is examining security issues at DOE and NNSA in the post-September 11 environment. Appendix I provides further details on our methodology.

² U.S. General Accounting Office, *NNSA Management: Progress in the Implementation of Title 32*, [GAO-02-93R](#) (Washington, D.C.: Dec. 12, 2001).

³ Additional initiatives were developed during this time period that were not related to nuclear security. For example, a number of initiatives related to energy sector critical infrastructure protection were developed that are not included in this report. Further, naval reactors developed several internal initiatives that are not included in this report, due to that program's semiautonomous status within NNSA.

⁴ Two nuclear security initiatives are not included in this report because the organizations affected by the initiatives either no longer exist or have indefinitely suspended operations.

Results in Brief

DOE and NNSA have made progress in implementing many of the 75 initiatives begun since 1998. Their experience with these initiatives highlights lessons to be learned that could improve implementation of future initiatives. DOE and NNSA have completed 64 percent of the initiatives, and most of the remaining initiatives are to be completed by December 2002. Successful implementation of the initiatives can enhance security at NNSA facilities. For example, DOE has eliminated the backlog of security clearance investigations and reinvestigations of employees with access to classified information. There are three lessons to be learned from implementing these initiatives that can help ensure future initiatives achieve their intended benefits.⁵ First, field perspectives should be fully considered in the development of initiatives. For example, DOE's new foreign visits and assignments database is incompatible with local databases at the two national laboratories we visited because field perspectives were not fully considered in the development of system specifications due to the fast track approach to implementing the initiative. Second, initiatives should be clearly communicated to the field. For example, contractor officials at one national laboratory received guidance on some cyber security initiatives from multiple offices within DOE and NNSA, often through informal means such as web site postings or verbal communication. This lack of clear communication produced confusion at sites about which requirements they needed to implement. Third, a coordinated process for implementing initiatives could be beneficial. The Pantex Plant developed such a process involving staff from all security areas. This contrasts with the two national laboratories where implementation was conducted primarily by staff in the security area most affected by the initiative rather than by the security team as a whole. Pantex officials told us that their process resulted in, among other things, identifying and avoiding unintended outcomes of implementation for certain initiatives. Therefore, it might serve as a best practice for other NNSA sites to consider. This report contains recommendations to the secretary of energy and the administrator of NNSA regarding these lessons to be learned so that future initiatives applicable to NNSA facilities can be more effectively developed and implemented.

⁵ These lessons to be learned do not pertain to the naval reactors program because of its unique security structure and program within NNSA. Bettis Atomic Power Laboratory had effectively implemented the initiatives that were applicable to it.

NNSA has begun to establish a security organization and program to safeguard nuclear information and materials, but several key issues still need to be addressed to ensure that the new security program is effective. NNSA has almost completed staffing the two new offices created to lead its security and counterintelligence activities and, with DOE, is completing a detailed review of security policies and procedures. NNSA has also initiated specific activities, including training, to create a security-oriented culture in its organization. Additionally, in response to the September 11 terrorist attacks, both headquarters and NNSA field sites have taken a number of short-term actions to improve security and have initiated other long-term activities aimed at strengthening their security structure and program. However, since NNSA's overall organizational structure is not completely functional, lines of authority for security oversight have not been clearly laid out. For example, a newly established office in NNSA—Facilities and Operations—has responsibility to oversee, among other things, implementation of safeguards and security programs and coordinate with NNSA field sites. However, it is not yet clear how the line of authority for security accountability in the field will be carried out regarding this office and existing NNSA operations and area offices. In addition, there is still confusion about the roles and authorities between DOE and NNSA security offices. For example, some contractor and NNSA field staff told us that they receive guidance from both DOE and NNSA security offices, resulting in confusion and uncertainty about which policies they are required to implement and which offices have authority over them. Finally, methods for evaluating the effectiveness of security are still being developed. These methods can lead to the establishment of security-related performance measures, which could assist in the preparation of the annual performance plan required by the Government Performance and Results Act of 1993. DOE's and NNSA's headquarters counterintelligence staffs have begun to develop methods for evaluating the effectiveness of their activities. NNSA's Office of Defense Nuclear Security has not yet begun to develop such methods because of higher priority work. However, it has incorporated some goals, strategic indicators, and performance measures into its strategic planning documents. DOE's Office of Security has a separate effort underway to produce new methods for assessing progress in its programs. Without these methods in place, DOE and NNSA cannot determine the impact of individual initiatives or the effectiveness of their security. While NNSA is addressing all these issues, clarifying who provides security direction and establishing clear lines of accountability from headquarters to the contractor for security activities as quickly as possible take on increased importance in the aftermath of the September 11 terrorist attacks. This

report contains a recommendation to ensure the development of an effective NNSA security structure and program.

In commenting on our draft report, DOE and NNSA concurred with all of our recommendations. They noted that the administrator's February 25, 2002, report to the Congress on NNSA's organization and operations includes plans pertinent to each of our recommendations. In our view, while there are promising elements of that report, it is only a framework for their eventual reorganization. It is not clear from DOE's and NNSA's comments how the February 25 report will address certain aspects of our recommendations. NNSA is developing a plan with milestones to guide the myriad details needed to successfully implement its reorganization. Including specific activities and corresponding time frames regarding our recommendations in this implementation plan would help ensure that they are effectively addressed.

Background

Several security incidents in the late 1990s highlighted the need for improvements at DOE. For example, the possible loss of nuclear weapons design information and the "missing" computer hard drives at Los Alamos National Laboratory revealed important weaknesses in security. More broadly, many reports have criticized DOE security: the President's Foreign Intelligence Advisory Board report,⁶ the Cox Committee report,⁷ and a number of our reports on particular aspects of DOE's security program.⁸ In response to individual events and reports, DOE, and later NNSA, developed initiatives intended to address nuclear security problems. Numerous initiatives were undertaken to strengthen, among other things, personnel, physical, information, and cyber security as well as DOE's counterintelligence program. Because of their importance, the initiatives were in many cases special efforts undertaken outside the established departmental processes for policy development, which include, among other things, the opportunity for all affected parties to review and comment on proposed policies.

⁶ President's Foreign Intelligence Advisory Board, *Science At Its Best, Security At Its Worst. A Report On Security Problems at the U.S. Department of Energy* (Washington, D.C.: June 1999).

⁷ Select Committee, United States House of Representatives, *U.S. National Security and Military/Commercial Concerns With The People's Republic Of China* (Washington, D.C.: May 1999, declassified report release date).

⁸ A list of related GAO products appears at the end of this report.

DOE and NNSA security activities associated with the initiatives generally fall under two major offices in each organization.⁹ For DOE headquarters, these are the Office of Security and the Office of Counterintelligence. The Office of Security is responsible for establishing policies and procedures to protect, among other things, nuclear materials and information at all DOE and NNSA facilities at headquarters and in the field. The Office of Counterintelligence is responsible for setting counterintelligence policy for DOE and NNSA, as well as gathering information and conducting activities to protect against espionage and other intelligence activities at non-NNSA sites. For NNSA, the two major offices are the Office of Defense Nuclear Security and the Office of Defense Nuclear Counterintelligence. These offices administer and manage security and counterintelligence functions within NNSA. Security activities are also carried out in the field at DOE and NNSA operations offices, area offices, laboratories, and production facilities.

NNSA's field structure includes national weapons laboratories, production facilities, and naval reactors program sites. Among the three national laboratories are Lawrence Livermore in California and Sandia in New Mexico, which conduct research and development for the nuclear weapons program and a broad range of nonnuclear research. The Pantex Plant in Texas is one of four production sites. Pantex assembles and disassembles nuclear weapons; stores nuclear weapons components on an interim basis; and develops, fabricates, and tests explosive components for nuclear weapons. The Bettis Atomic Power Laboratory in Pennsylvania is one of two naval reactor laboratories. Among other activities, Bettis conducts research, designs new reactor and propulsion systems, and provides technical expertise to the Navy's nuclear fleet.

⁹ Beyond the two major offices in each organization, other offices also have security implementation and oversight responsibilities, such as the Office of Independent Oversight and Performance Assurance and various program offices.

DOE and NNSA Have Implemented Many Initiatives, and Lessons Can Be Learned to Improve Future Initiatives

DOE and NNSA have implemented 64 percent of the 75 nuclear security initiatives developed since 1998. Of the remaining initiatives, most are to be completed by December 2002. Successful implementation of the initiatives can enhance security at NNSA facilities. There are three lessons to be learned from implementing these initiatives that can help ensure future initiatives achieve their intended benefits. First, field perspectives should be fully considered in the development of initiatives. Some initiatives, such as the development of a new foreign visits and assignments database, were developed without fully considering the perspectives of contractor and NNSA staff in the field, leading to operational inefficiencies and staff frustration. Second, initiatives should be clearly communicated to the field. Initiatives were not always clearly communicated to the field, resulting in confusion among contractor and NNSA field staff regarding what requirements they needed to implement. Third, a coordinated process for implementing initiatives could be beneficial. Some sites did not have a coordinated process for implementing initiatives, although at the Pantex Plant we observed a potential best practice in which a team approach for implementing initiatives had been developed. These lessons to be learned do not pertain to the naval reactors program because of its unique security structure and program within NNSA.¹⁰

Sixty-Four Percent of the Initiatives Have Been Implemented

DOE and NNSA have made progress in implementing the 75 nuclear security initiatives developed since 1998. As of January 2002, 48—or 64 percent—of the initiatives had been completed. DOE and NNSA report that 19 initiatives will be completed by December 2002 and that one will be completed in 2007. DOE and NNSA do not have expected completion dates for the remaining seven initiatives. Table 1 shows the general status of the initiatives, while appendix II provides details on the status of each initiative.

¹⁰ Bettis Atomic Power Laboratory had effectively implemented the initiatives that were applicable to it.

Table 1: Status of DOE/NNSA Security Initiatives

Status	Number	Percent
Complete	48	64
In progress	27	36
Total	75	100

Note: Not all of these initiatives applied to the naval reactors program. Appendix II identifies those initiatives that were not applicable to that program.

Source: GAO analysis of DOE and NNSA data.

Successful implementation of the initiatives can reduce the likelihood of security problems and therefore enhance security at NNSA facilities. For example, DOE has eliminated the backlog of security clearance investigations and reinvestigations of employees with access to classified information. Eliminating this backlog ensures that those employees with access to classified information have had their backgrounds checked and that cleared personnel needed in important mission-related areas are available for work. Other initiatives can strengthen controls over cyber security. For example, DOE has published 29 cyber security directives for classified and unclassified systems and has provided cyber security training for system administrators and managers. In addition, the counterintelligence program has been improved. For example, DOE and NNSA have integrated counterintelligence and foreign intelligence operational and analytic efforts throughout the nuclear weapons complex. This integration should lead to improved analyses by counterintelligence personnel at headquarters and in the field due to their increased access to the expertise of, and information available through, foreign intelligence staff.

DOE and NNSA have 27 initiatives that are still in progress. These initiatives address a broad range of security areas, including information security, physical security, nuclear material accountability and control, cyber security, and counterintelligence. According to DOE and NNSA, 19 of these initiatives will be completed by December 2002. Another initiative, intended to improve communication with employees regarding security, will be completed in 2007. DOE and NNSA could not provide specific completion dates for the remaining seven initiatives. Two of the seven are cyber security initiatives related to the implementation of a cyber security architecture program and the development of a research and development capability for DOE. As such, according to DOE officials, these initiatives represent continuous efforts. For the other five, DOE and NNSA officials told us they could not develop reasonable completion dates. For example,

DOE officials said that they do not have a completion date for the initiative to encrypt selected classified electronic media because they are waiting for the National Institute of Standards and Technology to provide a list of qualified vendors that meet the new advanced encryption standard.

**Experience to Date
Highlights Lessons to Be
Learned for Future
Initiatives**

Three lessons can be learned from DOE's and NNSA's experience in implementing the initiatives that can help ensure future initiatives achieve their intended benefits. First, field perspectives should be fully considered in the development of initiatives. Second, initiatives should be clearly communicated to the field. Third, a coordinated process for implementing initiatives could be beneficial.

**Field Perspectives Should Be
Fully Considered in the
Development of Initiatives**

Contractor and NNSA field staff at three sites told us that their perspectives were not fully considered in the development of initiatives. The initiatives were typically formulated at headquarters by security staff without full review, comment, or discussion from the field. In contrast, for proposed policies and directives, DOE and NNSA have a formal review and comment process in place, through which field staff can provide input. For example, according to contractor staff at the two national laboratories we visited, field perspectives on system specifications were not fully considered in the development of DOE's new foreign visits and assignments database. As a result, it is incompatible with local databases at these two sites. The volume of foreign interactions at these sites makes this problem significant. Because of the database incompatibilities, information must be manually entered into DOE's database by contractor staff at these sites, rather than being uploaded electronically. Further, at one of these sites, DOE's database is being used only on a limited basis because of these problems. Contractor officials at the two sites said that had they been involved more when this initiative was being developed, these problems might have been avoided or reduced. Office of Security officials admitted that participation by field staff was constrained by the fast track approach to implementation. However, these officials pointed out that since the database became operational, field staff have been actively included in continuing program development, system enhancement, and training activities.

Another example of difficulties caused by the lack of full consideration for field perspectives occurred in an initiative requiring a departmentwide inventory of electronic media containing certain classified information. This initiative required a complete inventory at all sites, within 30 days, of all electronic media containing certain classified information. Contractor officials at three sites told us that problems they experienced

Initiatives Should Be Clearly Communicated to the Field

implementing this initiative might have been foreseen and mitigated if field perspectives had been more fully considered in its development. For example, security staff at the three sites said that unclear wording in the initiative led to confusion and debate as to what media and information were actually covered by the initiative. Ultimately, staff at each site interpreted and implemented the initiative based on their local decisions as to its meaning and intent. Further, staff at two sites told us that the requirement to complete the inventory within 30 days was unrealistic given the quantity of affected media at their sites. As a result, their efforts were rushed and some aspects of the inventory, such as inaccurate reading of bar codes at one site, caused difficulties that they were still trying to resolve at the time of our visits.

Contractor and NNSA field staff at three sites told us that the initiatives were not always clearly communicated to them from headquarters. There was no systematic, uniform process in place for notifying sites of initiatives, and in some cases the initiatives were communicated through web sites, memorandums, and word of mouth.¹¹ For example, contractor officials at one national laboratory told us that multiple offices within DOE and NNSA provided guidance to them on some cyber security initiatives, often through informal means such as web site postings or verbal communication. This lack of clear communication produced confusion at the site about which requirements they needed to implement. In regard to two physical security initiatives, there is some confusion as to who is responsible for their completion. One of these initiatives addresses the hiring of additional security personnel and security maintenance technicians; the other addresses accelerating upgrades to physical safeguards and security. Headquarters states that these are primarily field initiatives, while contractor security staff at three sites we visited told us that they had received no guidance on or notification of these initiatives and did not know how the initiatives pertained to their sites. Although each of the sites had ongoing activities for improving physical security, the activities were not a result of the initiatives. Rather, the activities were an outcome of either internal site security assessments or external reviews by DOE's Office of Independent Oversight and Performance Assurance. In light of the attacks of September 11, 2001, both of these initiatives may be

¹¹ In commenting on communication between headquarters and the field, Office of Security officials told us that they have the Internet-based Directives System for posting new and established directives. It is important to note, however, that this system applies only to those initiatives that eventually become directives. Initiatives are not directly posted to this system.

A Coordinated Process for Implementing Initiatives Could Be Beneficial

of increased importance, and the need to clearly communicate to field sites the intended actions and outcomes associated with them is even more crucial.

Contractor and NNSA officials at Pantex have developed a formal, coordinated process for rapidly implementing initiatives as they are announced from headquarters. Under this process, as soon as site staff become aware of a new initiative, key contractor and NNSA officials from all security areas meet as a team to develop an initial implementation plan for the initiative. The team identifies all those individuals and offices that should be involved in implementation, the potential impacts on the overall security program, the best way to ensure that the initiative is implemented effectively, and the associated costs and other resource requirements. The result is early buy-in from all security areas regarding the site's implementation strategy, not just from the security area most affected by the initiative. Importantly, the development and successful use of this rapid implementation process has been formally incorporated into the Pantex site contract as a performance objective for the contractor. Pantex staff told us that this process has worked well for them and has allowed them to quickly respond to initiatives in a way that minimizes implementation problems. For example, they said that by using this process, Pantex was able to move more efficiently to determine a strategy for interpreting and implementing the required inventory of classified electronic media that caused more problems at other sites.

In contrast, at two field sites, implementation of initiatives was conducted primarily by contractor staff in the security area most affected by the initiatives, rather than with the coordinated input of staff from all security areas. While staff at these locations were generally able to implement the new requirements, a team approach involving staff with other areas of security expertise and responsibility might have helped identify more efficient or effective alternative implementation strategies. Further, this broader involvement might have provided insights into unintended outcomes of implementation for the overall security program and ways to avoid or minimize them. Therefore, the process at the Pantex Plant could be a potential best practice for other NNSA sites to consider.

NNSA Has Begun to Develop a Security Structure and Program, but Key Issues Need to Be Addressed

Since NNSA's creation, its officials have taken some steps to develop a security structure and program, including staffing offices, developing guidance, reviewing security policies and procedures, and initiating actions to create a security-oriented culture. Additionally, in response to the September 11 terrorist attacks, both headquarters and NNSA field sites have taken a number of short-term actions to improve security and have initiated other long-term activities aimed at strengthening their security structure and program. However, several key issues still need to be addressed to ensure an effective security structure and program. First, NNSA's overall organizational structure is not completely functional, including the newly established facilities and operations office, which is to oversee, among other things, implementation of NNSA's safeguards and security program and coordinate with field sites. Second, the roles and authorities between DOE and NNSA security offices have not been clearly articulated, resulting in confusion and uncertainty among contractor and NNSA field staff regarding what policies they are required to implement and which offices have authority over them. Third, methods for evaluating the effectiveness of security are still being developed, with NNSA's counterintelligence program just beginning to explore the development of such methods, and NNSA's security program not yet having begun such an effort because of other higher priorities.

Actions Have Been Taken to Establish a Security Structure and Program

NNSA officials have taken some steps to develop a security structure and program. In this regard, both the Office of Defense Nuclear Security and the Office of Defense Nuclear Counterintelligence have brought on staff to perform headquarters functions. As of January 2002, the Office of Defense Nuclear Security had reached its goal of 7 staff, including the chief, and the Office of Defense Nuclear Counterintelligence had filled 9 of its 11 staff positions, including the chief. Both offices have also begun developing guidance for implementing DOE policies and procedures at NNSA facilities. For example, Defense Nuclear Security has issued an initial "Implementation Bulletin" for DOE's Safeguards and Security Program order,¹² which provides guidance on how this order should be implemented at NNSA facilities. The order is the foundation for many security activities throughout the nuclear weapons complex. The issuance of the bulletin for this order was a needed first step toward adapting DOE policies for NNSA's use. The office's work on other implementation

¹² Department of Energy, *Safeguards and Security Program*, DOE O 470.1 (Washington, D.C.: Sept. 28, 1995).

bulletins was delayed by its focus on responding to the events of September 11. However, bulletins for some key safeguards and security areas are being drafted, with issuance expected by early spring of 2002.

NNSA, along with DOE, is also completing work associated with a comprehensive 6-month review of existing and draft security policies and procedures. The working teams that conducted the review were composed of headquarters and field staff, including federal and contractor employees. The working teams identified three categories of issues related to problem policies and procedures. These were (1) those about which there was confusion regarding implementation or interpretation, (2) those for which the language needed clarification or where minor policy changes were needed, and (3) those for which there was a fundamental difference of opinion among team members regarding appropriate departmental policy. To correct the identified problems, NNSA and DOE will address the policies and procedures in each of the three categories in different ways. Specifically, an NNSA implementation bulletin will be developed for each policy and procedure in the first category; the Field Management Council will review those in the second category;¹³ and a decision by the secretary of energy will be required for the third category, if a change is deemed appropriate. The report on the outcomes of this comprehensive review, and related recommendations, is still in draft form and has not yet been publicly released.

Along with these activities, NNSA has also initiated actions to create a security-oriented culture in its organization. For example, NNSA's and DOE's counterintelligence offices have completed a self-initiated communications effort to support counterintelligence awareness throughout NNSA and DOE. This effort included the completion of a comprehensive communications/awareness strategy and the establishment of a task force with membership from counterintelligence offices across the DOE/NNSA complex to monitor progress, share information, and maintain program momentum. The effort also included the development of a communications "tool kit," which was provided to all senior counterintelligence officers across the complex for use in their awareness presentations. These presentations are an ongoing part of routine counterintelligence program activities. Similarly, Defense Nuclear Security

¹³ The Field Management Council is composed of representatives from various DOE and NNSA staff and support activities, as well as line programs. The council is responsible for reviewing policies and requirements affecting the field.

has begun a self-initiated program called “Integrated Safeguards and Security Management.” Among the guiding principles of this program are individual responsibility for and participation in security, as well as line management responsibility for safeguards and security. The purpose of this program is to integrate security awareness into management and work practices at all levels and to ensure that all employees from management on down perceive security as a fundamental component of their day-to-day activities. The program should be fully implemented by the end of 2002.

According to NNSA officials, establishing an effective security structure and program is a long-term process. The chief of defense nuclear security described his program as “a work in progress” and told us that he envisions a 3-year process for program development. He said that the first year—in which he is currently working—entails solving problems, such as the organizational structure, and understanding the budget. The second year will focus on setting up the security budget process within NNSA and “winning the hearts and minds” of employees. The third year will involve assessing the previous 2 years’ actions and making corrections as needed. Similarly, the chief of defense nuclear counterintelligence told us that her program is still evolving and that fully establishing it will require various actions over the course of several years. Along with these internal plans and activities, the scope and direction of NNSA’s security structure and program may also be affected by external events such as the terrorist attacks of September 11. Because of this, it seems inevitable that new initiatives will be developed in the future that will affect program goals and directions.

In response to the September 11 terrorist attacks, both headquarters and NNSA field sites took a number of short-term actions to improve security. For example, immediately following the attacks, these NNSA facilities instituted a heightened state of alert, or security condition, in accordance with DOE orders.¹⁴ In conjunction with this heightened condition, security measures were enhanced to include additional barriers and access controls, increased vehicle searches, and increased patrols of perimeters and critical facilities. In addition, emergency operations centers at headquarters and in the field were staffed,¹⁵ and DOE and NNSA

¹⁴ DOE guidance on security conditions is contained in DOE Notice 473.6, approved September 18, 2000.

¹⁵ Emergency operations centers are facilities at headquarters and field sites that act as control centers for the overall management and direction of the sites’ emergency response activities.

headquarters security personnel provided threat advisories and security recommendations to field sites via complexwide videoconferences. Further, headquarters counterintelligence staff distributed information to field personnel on threats from foreign intelligence activities, and site counterintelligence officers provided briefings to site management and other employees on these threats. Counterintelligence staff also took steps to increase their liaison with outside agencies, including the Federal Bureau of Investigation.

As a result of the September 11 attacks, NNSA also began several long-term activities to strengthen its security structure and program. For example, the weekend after the attacks, NNSA initiated a vulnerability assessment of its high-risk targets. This “72-Hour Security Review” rated NNSA facilities against various criteria, including the possibility of nuclear detonation; radiological dispersion; and loss of program capability, technical staff, and life. In addition, as part of this review, each site was asked to identify vulnerabilities and the projected costs of correcting them. From this review, NNSA compiled a prioritized list of needed security improvements. In addition to this review, NNSA established a 90-day Combating Terrorism Task Force to review headquarters and field actions to protect NNSA interests. The task force has initiated work to revise a key DOE/NNSA security planning document—the Design Basis Threat.¹⁶ Other task force activities include site-by-site security review and vulnerability assessments, an assessment of nuclear materials management practices, and reviews of personnel security and transportation security. The director of security for the naval reactors program told us that his program’s actions since September 11 were consistent with those taken by DOE and the rest of NNSA. Naval reactors participated in the 72-Hour Security Review, and it is assessing identified vulnerabilities and determining requirements for short- and long-term actions.

¹⁶ The Design Basis Threat identifies and characterizes potential threats to DOE programs and facilities. Along with other security-related information, it is used in the design and implementation of protection programs and strategies.

Effectiveness Depends on Addressing Key Issues

Despite the actions that NNSA has already taken to develop a security structure and program, several key issues still need to be addressed to ensure that the structure and program is effective and to build upon the benefits of the initiatives. First, NNSA's overall security structure is not completely functional. Second, the roles and authorities between DOE and NNSA security offices have not been clearly articulated. Third, methods for evaluating the effectiveness of security are still being developed.

NNSA's Overall Security Structure Is Not Completely Functional

In May 2001, NNSA's administrator identified a proposed structure for his organization.¹⁷ This structure includes staff offices such as Defense Nuclear Security and Defense Nuclear Counterintelligence, program offices such as Defense Nuclear Nonproliferation and Defense Programs, and support offices such as Management and Administration and Facilities and Operations. However, in December 2001, we reported that a clearly delineated overall organizational structure still did not exist.¹⁸ In addition, during our review, headquarters staff, as well as contractor and NNSA field officials at three of the sites we visited, told us that NNSA's overall organizational structure is not completely functional. For example, the structure includes a new facilities and operations office to oversee, among other things, implementation of safeguards and security programs and coordinate with field sites.¹⁹ While the office was formally established in October 2001, it is not yet clear how the office will function with other NNSA offices. Of particular concern to some contractor and NNSA field staff is how the line of authority for security accountability will be carried out regarding this new office and existing NNSA operations and area offices. In this regard, staff were not sure which offices would be in charge of what activities, to whom contractor staff would report, and from whom contractors would receive direction. While contractor and NNSA field staff we spoke with were generally hopeful that the new facilities and operations office might be a positive step, a few were concerned that it might simply add another layer of bureaucracy to NNSA's organization. Other areas of uncertainty related to the facilities and operations office

¹⁷ National Nuclear Security Administration, *Report to Congress on the Plan for Organizing the National Nuclear Security Administration* (Washington, D.C.: May 3, 2001).

¹⁸ [GAO-02-93R](#).

¹⁹ According to NNSA and DOE officials, counterintelligence program activities and oversight will not be part of the facilities and operations office's functions. Counterintelligence has its own organizational reporting line and has an established organizational structure already in place.

**Roles and Authorities between
DOE and NNSA Security
Offices Have Not Been Clearly
Articulated**

included how the directors of NNSA's national laboratories would fit into this organizational structure and where security staff assigned to the office would be located (whether at headquarters or in the field). The chief of defense nuclear security, who will also temporarily be in charge of the security component within Facilities and Operations,²⁰ told us that his current plan calls for about 23 or 24 security staff, with some located in the field. He also told us that the mission and functions of the security component within Facilities and Operations are more clearly delineated in the administrator's progress report. As of February 1, 2002, this report was undergoing internal review.

Because of the broad scope and various locations of DOE and NNSA security activities, a clear understanding of roles and authorities between DOE and NNSA security offices is essential for an effective security program to be implemented at NNSA. However, some NNSA headquarters staff, as well as both contractor and NNSA field staff at three sites, told us that the roles and authorities between DOE and NNSA security offices have not been clearly articulated.

NNSA and DOE headquarters counterintelligence officials have a memorandum of understanding between their two offices that delineates their respective roles and authorities. However, contractor and NNSA field staff at two sites told us the memorandum has not worked in practice because they still receive direction from both offices, resulting in a sense in the field that they "serve two masters." The heads of the two counterintelligence offices told us that they recognize this problem and that they are working to develop additional guidance clarifying roles and authorities.

NNSA's Office of Defense Nuclear Security and DOE's Office of Security do not have any memorandum of understanding. According to the chief of defense nuclear security, he and DOE's director of security meet on a regular basis when resolution of issues is warranted. Further, he said that although no general memorandum of understanding is planned between the two offices, memorandums for specific areas such as classification might be developed. However, some contractor and NNSA field staff at two sites told us that they receive guidance from both NNSA and DOE security offices. This has resulted in confusion and uncertainty about

²⁰ The security component within Facilities and Operations is the Office of Nuclear Safeguards and Security Programs.

Methods for Evaluating the Effectiveness of Security Are Still Being Developed

which policies contractors and field staff are required to implement and which offices have authority over them. For example, NNSA security staff at one site said that contradictory input received from DOE and NNSA during the development of a fundamental security planning document—the Site Safeguards and Security Plan—led to confusion and frustration regarding what needed to be done in order to have the document approved. Further, these staff told us that they questioned why DOE was involved in the process at all, since their understanding was that NNSA has sole responsibility for implementing security policies in the field. The chief of defense nuclear security told us that the security component of the newly established facilities and operations office is expected to help address this type of problem in the future.

Methods for evaluating security, both qualitative and quantitative, provide a way to assess the effectiveness of, and improvements in, all aspects of the security program. NNSA and DOE officials do not yet have such methods in place. Without these methods, NNSA and DOE cannot determine the impact of individual initiatives or the effectiveness of their security. These evaluation methods can also lead to the establishment of security-related performance measures, which could assist the agencies in preparing the annual performance plan required by the Government Performance and Results Act of 1993. In this regard, we have identified problems with DOE's security-related performance measures in its annual performance plan.²¹ Specifically, some performance measures DOE has been using do not really assess the overall effectiveness of security or improvements in performance. Rather, these measures are process-oriented, focusing on whether specific security activities are carried out.

NNSA's and DOE's counterintelligence offices have begun to jointly explore the creation of a set of metrics for evaluating the effectiveness of their activities. In this regard, they have been working with Department of Defense counterintelligence officials to learn from and establish benchmarks against that agency's program. Additionally, they plan to involve contractor and NNSA field staff in this effort. NNSA and DOE counterintelligence officials told us that, presently, their program cannot assess the value added from an activity. Eventually, they hope that they will be able to evaluate effectiveness and improvements in all aspects of

²¹ U.S. General Accounting Office, *Department of Energy: Status of Achieving Key Outcomes and Addressing Major Management Challenges*, GAO-01-823 (Washington, D.C.: June 29, 2001).

their program. These officials also said that their metrics development effort should take several years to complete. NNSA's Office of Defense Nuclear Security has not yet begun to develop such methods because of higher priority work. However, it has incorporated some goals, strategic indicators, and performance measures into its strategic planning documents. The chief of this office told us that methods for assessing the progress of his program are at least a year away and that the methods will likely be qualitative rather than quantitative in nature. He further told us that approaches to evaluating his security program are likely to change due to world events. DOE's Office of Security has a separate effort underway to produce new metrics for evaluating progress in its programs. This effort initially focused on cyber security but was expanded to include the full range of DOE security activities overseen by this office such as physical, personnel, and information security. As with NNSA's efforts, DOE officials expect their metrics development process to be a long-term undertaking.

Conclusions

The terrorist attacks of September 11, 2001, bring into sharp focus the necessity for all federal agencies to take seriously threats to their assets. In light of these attacks, agency efforts to enhance security take on even greater urgency, especially in relation to the protection of assets in the nation's nuclear weapons complex. DOE and NNSA have made progress in implementing many of the nuclear security initiatives developed since 1998. There are lessons to be learned from the implementation of these initiatives. These lessons can be very important for any initiatives stemming from the September 11 attacks. Involving contractor and NNSA field staff in the development of new initiatives, communicating them clearly to those charged with implementation, and establishing coordinated processes at field sites to implement new requirements would enhance NNSA's ability to quickly and effectively institute new security activities.

NNSA has also made progress in developing a security structure and program. As noted in this report, for this structure and program to be most effective, NNSA must ensure that its overall organizational structure is fully functional, clarify roles and authorities, and continue its efforts to develop methods for evaluating program effectiveness and improvement. NNSA has recognized these issues and has efforts underway to make the overall organizational structure fully functional and develop methods for evaluating the effectiveness of the security program. Nevertheless, both NNSA and DOE could benefit from clarifying the roles and authorities of various security offices.

Recommendations for Executive Action

We are making recommendations to the secretary of energy and the NNSA administrator aimed at ensuring that the lessons to be learned from prior initiatives are incorporated into the development and implementation of future initiatives. We are also making a recommendation to better ensure the development of an effective NNSA security structure and program.

- Ensure that contractor and NNSA field staff are substantively involved in the development of security initiatives and that such initiatives are clearly communicated to the field.
- Consider requiring NNSA field sites to develop a coordinated implementation process that would allow contractor and NNSA staff to quickly address and implement initiatives, using the team approach followed at the Pantex Plant as a potential best practice for other sites.
- Clearly define roles and authorities of DOE and NNSA security and counterintelligence offices to ensure that contractors and NNSA field staff understand what policies they are required to implement and which offices have authority over them.

Agency Comments and Our Evaluation

We provided DOE and NNSA with a draft of this report for review and comment. They concurred with all three of our recommendations. They believe that many elements of the NNSA administrator's recently issued February 25, 2002, report to the Congress on the organization and operations of NNSA will address our recommendations. In our view, while there are promising elements of that report, such as establishing clear lines of authority between NNSA and its contractors and promising to hold federal staff and contractors more accountable for performing NNSA's missions, it is only a framework for their eventual reorganization. Accordingly, it is not clear from DOE's and NNSA's comments how the February 25 report will address certain aspects of our recommendations. For example, we are recommending that NNSA consider requiring its field sites to develop a coordinated implementation process to respond to security initiatives that modeled what we saw at Pantex. The comments from DOE and NNSA note that the new organizational structure will allow for dynamic interaction to achieve goals quickly. It is not clear how this responds to our recommendation. Further, we are recommending that there be clearly defined roles and authorities of DOE and NNSA security offices. The comments imply that the organizational structure and functions laid out in the February 25 report will clarify for field staff the roles and authorities of the separate security offices in DOE and NNSA. However, the report does not address some of the issues we identified through our work regarding how DOE and NNSA security offices interact and function together. NNSA is developing a plan with milestones to guide the myriad details needed to successfully implement its reorganization.

Including specific activities and corresponding time frames regarding our recommendations in this implementation plan would help ensure that they are effectively addressed.

DOE and NNSA also made a general comment related to the process used at Lawrence Livermore National Laboratory for implementing security initiatives. They stated that Livermore's process, while less formalized than the one at Pantex, is coordinated, integrated, effective, and successful. We agree that Livermore's process has been successful, but we believe that a more formal coordinated process such as that used at Pantex would be beneficial for Livermore and others to consider. In our view, the process at Pantex provides the greatest assurance that initiatives will be implemented in the most effective and efficient manner, with the highest level of accountability. Finally, DOE and NNSA made specific comments of a technical nature that we incorporated as appropriate. DOE's and NNSA's comments are provided in appendix III.

To address our objectives, we interviewed officials and obtained documents from DOE, NNSA, and contractor officials. Further, we visited DOE and NNSA headquarters, as well as selected NNSA field sites. Our scope and methodology are discussed in detail in appendix I. We performed our review from January 2001 through January 2002 in accordance with generally accepted government auditing standards.

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this letter. At that time, we will send copies of the report to the secretary of energy, the administrator of NNSA, the director of the Office of Management and Budget, and appropriate congressional committees. We will make copies available to others on request.

If you or your staff have any questions about this report, please call me at (202) 512-3841. Major contributors to this report were William F. Fenzel, assistant director; Christopher M. Pacheco, senior analyst; and Frank B. Waterous, senior analyst.

A handwritten signature in black ink that reads "Gary L. Jones". The signature is written in a cursive style with a large, stylized "G" and "J".

(Ms.) Gary L. Jones
Director, Natural Resources
and Environment

Appendix I: Scope and Methodology

To determine the extent to which Department of Energy (DOE) and National Nuclear Security Administration (NNSA) security initiatives had been implemented at NNSA facilities, we worked with DOE and NNSA headquarters offices to develop a comprehensive list of all nuclear security initiatives since 1998. The primary offices with which we worked were DOE's Office of Security and Office of Counterintelligence and NNSA's Office of Defense Nuclear Security and Office of Defense Nuclear Counterintelligence.

We identified 75 nuclear security-related initiatives based on our review of presidential decision directives, announcements by the secretary of energy or other high-ranking department officials, and initiatives begun by DOE and NNSA security offices between February 1998 and January 2001. We excluded from our review several other initiatives from this time period because they did not relate to nuclear security, they were begun by and pertained only to the unique naval reactors program, or they were no longer applicable because the organizations affected by them either no longer existed or had indefinitely suspended operations. We did not assess whether these 75 initiatives addressed all security problems at DOE and NNSA. For the 75 initiatives, we asked NNSA and DOE to provide us with information on the status of, and actions or plans associated with, each. For those initiatives identified as completed, we collected documents and interviewed officials to independently verify their completion.

We also visited selected field sites that are representative of the various aspects of NNSA's work to determine whether the initiatives requiring field implementation were in place at these sites. Specifically, we visited Lawrence Livermore National Laboratory in California, Sandia National Laboratories in New Mexico, the Pantex Plant in Texas, and the Bettis Atomic Power Laboratory in Pennsylvania. Livermore and Sandia are national laboratories, Pantex is a production facility, and Bettis is a naval reactors program site. At each location, we met with both federal and contractor officials, obtained pertinent supporting documentation, and verified through physical observation and other means the extent of implementation.

To determine the extent to which NNSA has developed an organizational structure for security and a program to safeguard nuclear information and materials, we interviewed DOE and NNSA headquarters officials, as well as NNSA and contractor officials in the field. We also reviewed policy and planning documents, including orders, implementation guidance, and reports. We collected information on actions taken by DOE and NNSA in

response to the September 11 terrorist attacks, but we did not evaluate the implementation of these actions.

Appendix II: Status of Initiatives to Improve Nuclear Security at DOE and NNSA

Initiative	Status
February 1998	
Establish Foreign Visits & Assignments (FV&A) Office. ^a	Completed.
Establish a separate counterintelligence office, reporting directly to the secretary. ^a	Completed.
Require the director of counterintelligence to be a senior executive from the Federal Bureau of Investigation (FBI) and to staff his office with counterintelligence professionals. ^a	Completed.
Ensure that the director of counterintelligence will have direct access to the secretary of energy, the Central Intelligence Agency director, and the FBI director. ^a	Completed.
Make laboratory directors directly accountable to the secretary for performance of their counterintelligence programs. Amend laboratory contracts to include counterintelligence program goals and objectives.	Actions to amend contracts and finalize order are in progress. Contracts are expected to be amended once the draft order is signed by the secretary of energy, anticipated in early 2002.
Ensure that laboratory counterintelligence personnel have direct access to laboratory directors and concurrently report to DOE's counterintelligence director.	Completed.
Transfer DOE counterintelligence oversight from operations and field offices to headquarters.	Completed.
Prepare, within 90 days of the director's arrival, a report to the secretary to include a strategic plan for achieving long-term goals and recommendations on strengthening the counterintelligence program. ^a	Completed.
Initiate an internal inspection process to review annually the counterintelligence program and provide results to the secretary.	Completed.
Integrate counterintelligence and foreign intelligence operational and analytic efforts throughout DOE and the laboratories. ^a	Completed.
Develop and implement specific security measures to reduce the threat to classified and sensitive information at DOE, its field activities, and the laboratories.	Actions related to identification and protection of sensitive unclassified information are in progress. Completion is expected in early 2002.
Advise the assistant to the president for national security affairs, within 120 days, on the actions taken and specific remedies designed to implement Presidential Decision Directive 61. ^a	Completed.
May 1998	
Appoint departmental officials to be responsible for internal critical infrastructure protection. ^a	Completed.
Develop a plan, no later than 180 days from the issuance of this directive, for protecting the department's critical infrastructure, including, but not limited to, its cyber-based systems. ^a	Completed.
March 1999	
Develop counterintelligence Inquiry Management and Analysis Capability pilot program. ^a	Completed.
Impose stricter document controls at the laboratories for all secret and top secret documents that contain weapon design data. ^a	Actions to update order are still in progress. Completion is expected in March 2002.
Monitor implementation of counterintelligence plan. ^a	Actions to complete outstanding recommendations are in progress. Completion is expected in early 2002.
Review counterintelligence investigative files. ^a	Actions to review additional files are in progress. Completion is expected in 2002.
Report annually to the Congress on counterintelligence program. ^a	Completed.
Conduct classified counterintelligence internal inquiry. ^a	Completed.

**Appendix II: Status of Initiatives to Improve
Nuclear Security at DOE and NNSA**

Initiative	Status
Hire additional security personnel and security maintenance technicians. ^a	DOE headquarters officials state that this is a field initiative. However, field sites we visited had not been tasked with actions related to it. Initiative is currently on hold pending receipt of additional budget authority. DOE/NNSA did not provide an expected completion date for this initiative.
Improve and test plans to recover special nuclear materials in the unlikely event they are diverted. ^a	DOE/NNSA did not provide information on the status or the expected completion of this initiative.
Finalize efforts to ensure that materials accounting systems are accurate. ^a	Actions to expand and upgrade materials accounting systems are in progress. Completion is expected by fiscal year 2002.
Eliminate the backlog of reinvestigations of existing security clearances.	Completed.
Establish a counterintelligence and security team to make inspection visits to the five national security laboratories (Los Alamos, Lawrence Livermore, Sandia, Oak Ridge, and Pacific Northwest national laboratories). ^a	Completed.
Order an interim security review in July of the three operations rated marginal. ^a	Completed.
Increase the fiscal year 2000 budget request by \$8 million to better protect cyber systems. ^a	Completed.
May 1999	
Establish Office of Security and Emergency Operations. ^a	Completed.
Establish Office of Plutonium, Uranium and Special Material Inventory. ^a	Actions to bring staffing up to approved levels are in progress. Completion is expected by fiscal year 2002.
Establish Zero Tolerance Security Policy. ^a	Completed.
Accelerate actions that must be taken by DOE nuclear sites to remedy less than satisfactory ratings in the 1997/98 annual report to the president on safeguards and security at defense nuclear facilities. ^a	Ratings have improved since 1997/1998 and additional actions are in progress. DOE/NNSA did not provide information on the expected completion date of this initiative.
Accelerate upgrades to physical safeguards and security. ^a	Actions related to headquarters upgrades are in progress and scheduled for completion in fiscal year 2002. DOE headquarters states that NNSA and program offices are responsible for field upgrades. However, field sites we visited had not been tasked with actions related to this initiative. Nevertheless, the sites had ongoing activities related to physical security upgrades that they were prioritizing with input from NNSA's Office of Defense Nuclear Security.
Extend the automatic declassification deadline of Executive Order 12958 by 18 months. ^a	Completed.
Develop cyber security policies for classified and unclassified systems.	Twenty-nine directives were published from fiscal years 1999 through 2001. Actions to develop 10 additional directives are in progress. Completion is expected in December 2002.

**Appendix II: Status of Initiatives to Improve
Nuclear Security at DOE and NNSA**

Initiative	Status
Establish departmentwide computer security training program for personnel with cyber security responsibilities.	Training provided for system administrators/managers. Actions to provide further training and restructure/revise classified computer awareness courses are in progress. Completion is expected in September 2002.
Implement cyber security architecture program for the operation of existing systems and the development of future systems.	Actions to continue departmentwide cyber security infrastructure upgrades are in progress. DOE states that the expected completion date is not relevant since this is a continuous effort.
Attain research and development capability to research innovative cyber security protection capabilities and technology. ^a	Actions to continue this research are in progress. DOE states that there is no completion date for this initiative since it is an ongoing effort.
Request additional \$50 million over fiscal years 2000 and 2001 to support additional cyber security improvements. ^a	Completed.
Create a new Office of Independent Oversight and Performance Assurance to independently evaluate emergency and security operations. ^a	Completed.
End the backlog of all DOE background investigations. By the end of 1999, initiate all outstanding reinvestigations.	Completed.
Mandate the use of "banners" across the complex to alert users logging onto a system that they are operating on a government computer system subject to search and review.	Completed.
Establish counterintelligence vulnerability assessment group ("Red Team") to evaluate espionage threat and vulnerability and conduct counterintelligence/security program tests. ^a	Completed.
Require all facilities to use intrusion detection tools and report all intrusions to counterintelligence and the FBI's National Infrastructure Protection Center for investigation and analysis.	Actions to determine the scope of implementation are in progress. Completion is expected in 2002.
Sign memorandum of agreement between DOE and the FBI to ensure better coordination on DOE security and counterintelligence operations and FBI espionage investigations. ^a	Completed.
Notify DOE officials responsible for maintaining Q clearances and the Office of Counterintelligence of any issue that might impact the issuance and maintenance of such a clearance.	Completed.
Mandate reporting by employees of contacts with foreign nationals from sensitive countries.	Completed.
June 1999	
Conduct security awareness stand-downs at the three weapons laboratories. ^a	Completed.
July 1999	
FV&A Notice and Policy. ^a	Actions to finalize the order are in progress. DOE did not provide an expected completion date for this initiative.
Establish an FV&A database. ^a	Completed.
Conduct departmentwide security stand-down for day-long program of security training and education.	Completed.
August 1999	
Establish consolidated security budget. ^a	Completed.

**Appendix II: Status of Initiatives to Improve
Nuclear Security at DOE and NNSA**

Initiative	Status
October 1999	
Impose moratorium on DOE sensitive country nationals to weapons laboratories. ^a	Completed.
December 1999	
Issue final rules governing the use of polygraph examinations to support counterintelligence and security activities at DOE. ^a	Completed.
June 2000	
Review Nuclear Emergency Search Team (NEST) operations the same as other departmental programs. ^a	Completed.
Enhance verification procedures of authorized personnel access to vaults to record duration and time of access. ^a	Completed.
Man all vaults, and when not manned, lock and set alarms. ^a	Completed.
Have responsible operations/field offices conduct, within 30 days, a comprehensive evaluation of vault procedures with recommendations for policy and procedural improvements across the DOE complex. ^a	Actions to update physical security policies are in progress. Completion is expected in early 2002.
Encrypt selected classified electronic media. ^a	Actions are in progress, but on hold until the National Institute of Standards and Technology provides DOE a list of qualified vendors that meet the new Advanced Encryption Standard. Until that time, DOE has implemented interim encryption measures. DOE states that an expected completion date is unknown at this time.
Increase security requirements (higher protection level) mandated for classified encyclopedic databases. ^a	Actions to complete the requirements are in progress. DOE states that this initiative has been subsumed by the NNSA "higher fences" initiative. Completion is expected in March 2002.
Complete a DOE-wide mandatory inventory, within 30 days, for electronic media containing compendia of classified information such as that contained on the missing hard drives. ^a	Completed.
Conduct an inventory of all NEST and Accident Response Group databases within 10 days. ^a	Completed.
Have the Office of Independent Oversight and Performance Assurance inspect administrative security controls at the laboratories. ^a	Completed.
August 2000	
Establish FV&A Policy Review Team. ^a	Completed.
January 2001	
Charter an implementation review conference to assess the impacts of existing security and counterintelligence orders on the scientific and security environment at the laboratories. ^a	Actions to finalize the implementation review conference draft report are in progress. Completion is expected in 2002.
Self-initiated by specific programs/offices	
Increase security at NNSA via "Higher Fences" Program (Defense Nuclear Security initiative). ^a	Actions to finalize program are in progress. Completion is expected in March 2002.
Clarify security roles and responsibilities (Defense Nuclear Security initiative). ^a	Actions to define roles and responsibilities are in progress. Completion is expected in early 2002.
Establish the Integrated Safeguards and Security Management initiative/personnel education initiative (Defense Nuclear Security initiative). ^a	Actions to involve management are in progress. Completion is expected in 2002.
Implement security reforms at Los Alamos National Laboratory Technical Area 18 (Defense Nuclear Security initiative). ^a	Actions to continue next phase are in progress. Completion is expected in 2002.

**Appendix II: Status of Initiatives to Improve
Nuclear Security at DOE and NNSA**

Initiative	Status
Develop communications initiative (Defense Nuclear Security initiative). ^a	Actions to develop long-range plan and acquire funding are in progress. Completion is expected in 2007.
Develop and implement a counterintelligence collections program within DOE responsive to community collection requirements and supporting DOE analytical requirements (Office of Counterintelligence initiative). ^a	Completed.
Develop communications initiative specifically to support counterintelligence awareness throughout DOE and NNSA (Office of Counterintelligence initiative). ^a	Completed.
Update and improve the Counterintelligence Analytical Research Data System database (Office of Counterintelligence initiative). ^a	Actions to update and improve the database, such as migrating it to a web-based system, are in progress. Completion is expected in October 2002.
Create Counterintelligence Training Academy (Office of Counterintelligence initiative). ^a	Completed.
Develop Foreign Interactions Training Academy in Albuquerque, New Mexico (Foreign Visits and Assignments Office initiative). ^a	Completed.
Develop foreign visits and assignments "facilitator concept" (Foreign Visits and Assignments Office initiative). ^a	Completed.

^aInitiatives not applicable to the naval reactors program.

Appendix III: Comments from the Department of Energy and the National Nuclear Security Administration



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

MAR 11 2002

Ms. Gary L. Jones
Director, Natural Resources
and Environment
U. S. General Accounting Office
Washington, D.C. 20548

Dear Ms. Jones:

The General Accounting Office's draft report GAO-02-358, "NUCLEAR SECURITY: Lessons to Be Learned from Implementing NNSA's Security Enhancements," was reviewed by my office. The General Accounting Office (GAO) was requested to review the National Nuclear Security Administration's (NNSA) progress in implementing initiatives to improving security. Specifically, the GAO was asked to examine the extent to which (1) DOE and NNSA have implemented security initiatives at NNSA facilities and (2) NNSA has developed an organizational structure for security and a program to safeguard nuclear information and materials.

The report mentions NNSA being a semi-autonomous entity within DOE. For clarity's sake, the NNSA Act established a separately organized agency within DOE and gave the Administrator the authority over, and responsibility for, all programs and activities of the Administration. In his February 25, 2002, Report to Congress on the Organization and Operations of the National Nuclear Security Administration, the Administrator defined the Strategic Plan and the strategy for improving the organization's effectiveness and efficiency. That report provided DOE with the authority to provide independent oversight and performance assurance of safeguards and security—based on NNSA and other applicable standards—as well as the authority and oversight for personnel security and classification.

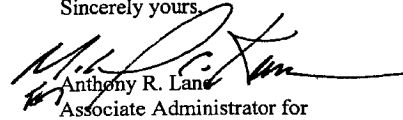
The new organizational functions and field structure now clarify roles and responsibilities; integrates and balances program elements; streamlines operations and oversight; and simplifies requirements. Guidance, direction, and control will only be provided to field and program elements by NNSA Headquarters thereby eliminating some of the confusion on the part of field elements.



Printed with soy ink on recycled paper

While we appreciate the many positive comments in the GAO draft report, we also want to reiterate that the NNSA organization is a work-in-process. We believe that the actions taken to date and the reengineering that is underway will enhance efficiency and effectiveness, enhance discipline and accountability, and reduce federal staffing for the organization, writ large, not just the security and counterintelligence community.

Sincerely yours,


Anthony R. Lane
Associate Administrator for
Management and Administration

Attachment

cc: Director, Office of Management, Budget and Evaluation/
Chief Financial Officer
Director, Office of Security and Emergency Operations

**Comments on
GAO Draft Report, GAO-02-358
“NUCLEAR SECURITY: Lessons to Be Learned from
Implementing NNSA’s Security Enhancements”**

General Comments

The National Nuclear Security Administration appreciated the opportunity to review and comment on the draft report. We believe the report to be factual and the recommendations reasonable. We would like to point out that the Lawrence Livermore National Laboratory process for implementing security initiatives, while less formalized than the system at Pantex is coordinated, integrated, effective, and successful. Livermore laboratory, as with other elements, has committees and working groups composed of representatives from key organizations to address security issues and facilitate the implementation of initiatives.

Specific Comments

Page 1. The second paragraph mentions the fact that Congress established the NNSA and the NNSA established the Offices of Defense Nuclear Counterintelligence and Defense Nuclear Security. In fact, the NNSA Act established all three offices.

Page 3. Footnote #5 should read “These lessons to be learned do not pertain to the Naval Reactors Program because they had effectively implemented the initiatives applicable to them.”

Page 5. The Office of Counterintelligence is responsible for, “<insert: setting of CI policy for DOE and NNSA> . . . gathering information and conducting activities to protect against espionage and other intelligence activities <insert: at non-NNSA sites>.”

Page 6. The statement is made that the Security and Counterintelligence offices in NNSA does not have responsibility to develop policy. In fact, the counterintelligence program has a jointly managed [DOE/NNSA] staff at Headquarters.

Page 6. The 5th sentence of the second paragraph should read “The Bettis Atomic Power Laboratory in Pennsylvania is one of two naval reactor laboratories.”

Recommendations for Executive Action

Recommendation 1

“Ensure that contractor and NNSA field staff are substantively involved in the development of security initiatives and that such initiatives are clearly communicated to the field.”

Now on page 6.

Management Comment

Concur

In his February 25, 2002, Report to Congress on the Organization and Operations of the National Nuclear Security Administration, the Administrator defined the Strategic Plan and the strategy for improving the organization's effectiveness and efficiency. In that report, the Administrator has established the Headquarters element to provide program direction and the site offices and labs and plants to provide program execution. This concept allows for clear expectations on the part of the field and measurable deliverables on the part of Headquarters. Additionally, Headquarters is working closely with field sites to insure their views are appropriately included in strategic plans and policy.

Recommendation 2

"Consider requiring NNSA field sites to develop a coordinated implementation process that would allow contractor and NNSA staff to quickly address and implement initiatives, using the team approach."

Management Comment

Concur

As stated in Recommendation 1, Headquarters provides program direction and the site offices and labs and plants provide program execution. This concept not only allows for clear expectations on the part of the field and measurable deliverables on the part of Headquarters but, allows for dynamic interaction to achieve goals quickly. An example of that is the counterintelligence office at Pantex and the integrated approach used to address issues.

Recommendation 3

"Clearly define roles and authorities of DOE and NNSA security and counterintelligence offices to ensure that contractors and NNSA field staff understand what policies they are required to implement and which offices have authority over them."

Management Comment

Concur

In his February 25, 2002, Report to Congress on the Organization and Operations of the National Nuclear Security Administration, the Administrator defined the Strategic Plan and the strategy for improving the organization's effectiveness and efficiency. That report provided DOE with the authority to provide independent oversight and performance assurance of safeguards and security-based on NNSA and other applicable standards—as well as the authority and oversight for personnel security and classification. The new organizational functions and field structure now clarify roles and responsibilities; integrates and balances program elements; streamlines operations and oversight; and simplifies requirements. Guidance, direction, and control will only be provided to field and program elements by NNSA Headquarters thereby eliminating some of the confusion on the part of field elements. There are formalized procedures for the counterintelligence community that define the roles and responsibilities for all parties. The counterintelligence strategic plan and the counterintelligence order formalizes all roles and responsibilities

Related GAO Products

Department of Energy: Fundamental Reassessment Needed to Address Major Mission, Structure, and Accountability Problems. [GAO-02-51](#). Washington, D.C.: December 21, 2001.

NNSA Management: Progress in the Implementation of Title 32. [GAO-02-93R](#). Washington, D.C.: December 12, 2001.

Nuclear Security: DOE Needs to Improve Control Over Classified Information. [GAO-01-806](#). Washington, D.C.: August 24, 2001.

Department of Energy: Views on the Progress of the National Nuclear Security Administration in Implementing Title 32. [GAO-01-602T](#). Washington, D.C.: April 4, 2001.

Information Security: Safeguarding of Data in Excessed Department of Energy Computers. [GAO-01-469](#). Washington, D.C.: March 29, 2001.

Major Management Challenges and Program Risks: Department of Energy. [GAO-01-246](#). Washington, D.C.: January 2001.

Nuclear Security: Information on DOE's Requirements for Protecting and Controlling Classified Documents. [T-RCED-00-247](#). Washington, D.C.: July 11, 2000.

Department of Energy: National Security Controls Over Contractors Traveling to Foreign Countries Need Strengthening. [RCED-00-140](#). Washington, D.C.: June 26, 2000.

Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research. [AIMD-00-140](#). Washington, D.C.: June 9, 2000.

Department of Energy: Views on Proposed Civil Penalties, Security Oversight, and External Safety Regulation Legislation. [T-RCED-00-135](#). Washington, D.C.: March 22, 2000.

Nuclear Security: Security Issues at DOE and Its Newly Created National Nuclear Security Administration. [T-RCED-00-123](#). Washington, D.C.: March 14, 2000.

Department of Energy: Views on DOE's Plan to Establish the National Nuclear Security Administration. [T-RCED-00-113](#). Washington, D.C.: March 2, 2000.

Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight. [RCED-00-62](#). Washington, D.C.: February 24, 2000.

Department of Energy: Need to Address Longstanding Management Weaknesses. [T-RCED-99-255](#). Washington, D.C.: July 13, 1999.

Department of Energy: Key Factors Underlying Security Problems at DOE Facilities. [T-RCED-99-159](#). Washington, D.C.: April 20, 1999.

Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Its Weapons Laboratories. [T-RCED-99-28](#). Washington, D.C.: October 14, 1998.

Department of Energy: Problems in DOE's Foreign Visitor Program Persist. [T-RCED-99-19](#). Washington, D.C.: October 6, 1998.

Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories. [RCED-97-229](#). Washington, D.C.: September 25, 1997.

DOE Security: Information on Foreign Visitors to the Weapons Laboratories. [T-RCED-96-260](#). Washington, D.C.: September 26, 1996.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily e-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
P.O. Box 37050
Washington, D.C. 20013

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

Visit GAO's Document Distribution Center

GAO Building
Room 1100, 700 4th Street, NW (corner of 4th and G Streets, NW)
Washington, D.C. 20013

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm,
E-mail: fraudnet@gao.gov, or
1-800-424-5454 or (202) 512-7470 (automated answering system).

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G. Street NW, Room 7149,
Washington, D.C. 20548